CLAIMS

WHAT IS CLAIMED:

1. A communications system, comprising:

physical layer hardware adapted to communicate data over a communications channel, the physical layer being adapted to demodulate an incoming analog signal to generate a digital receive signal and modulate a digital transmit signal to generate an analog transmit signal; and

a processing unit adapted to load a secure driver for interfacing with the physical layer hardware, the secure driver including program instructions for implementing a protocol layer to decode the digital receive signal and encode the digital transmit signal.

2. The system of claim 1, wherein the secure driver comprises a digitally signed file.

3. The system of claim 1, wherein the communications system includes a secure program storage device adapted to store the secure modem driver.

4. The system of claim 3, wherein the secure program storage device comprises a flash memory.

5. The system of claim 3, wherein the processing unit comprises a computer.

6. The system of claim 5, wherein the computer includes:

a processor complex adapted to execute the program instructions in the secure driver;

a bus coupled to the processor complex; and

an expansion card coupled to the bus, the expansion card including the physical layer hardware.

7. The system of claim 6, wherein secure program storage device is located on the expansion card.

8. The system of claim 6, wherein secure program storage device is located in the computer.

9. The system of claim 6, wherein the computer includes a system basic input output system (BIOS) memory adapted to store the secure driver.

10. The system of claim 2, wherein the communications system includes a program storage device adapted to store a public key for authenticating the digitally signed file.

11. The system of claim 2, wherein the processing unit comprises a computer having a system basic input output system (BIOS) memory adapted to store a public key for authenticating the digitally signed file.

12. The system of claim 3, wherein the secure program storage device is secured by an authentication key.

13. The system of claim 12, wherein the physical layer hardware is adapted to receive the authentication key over the communications channel.

14. The system of claim 3, wherein the secure program storage device is secured by a password.

15. A computer system, comprising:

a processor complex adapted to adapted to load a secure driver including program instructions for implementing a communications protocol;

a bus coupled to the processor complex; and

an expansion card coupled to the bus, the expansion card including physical layer hardware adapted to communicate data over a communications channel, the physical layer being adapted to demodulate an incoming analog signal to generate a digital receive signal and modulate a digital transmit signal to generate an analog transmit signal, wherein the secure driver interfaces with the physical layer hardware to decode the digital receive signal and encode the digital transmit signal.

16. The computer system of claim 15, wherein the secure driver comprises a digitally signed file.

17. The computer system of claim 15, further comprising a secure program storage device adapted to store the secure modem driver.

18. The computer system of claim 17, wherein the secure program storage device comprises a flash memory.

19. The computer system of claim 17, wherein secure program storage device is located on the expansion card.

20. The computer system of claim 15, further comprising a computer basic input output system (BIOS) memory adapted to store the secure driver.

21. The computer system of claim 16, further comprising a program storage device adapted to store a public key for authenticating the digitally signed file.

22. The computer system of claim 16, further comprising a system basic input output system (BIOS) memory adapted to store a public key for authenticating the digitally signed file.

23. The computer system of claim 17, wherein the secure program storage device is secured by an authentication key.

24. The computer system of claim 23, wherein the physical layer hardware is adapted to receive the authentication key over the communications channel.

25. The computer system of claim 17, wherein the secure program storage device is secured by a password.

26. A computer system, comprising:

a peripheral device; and

a processor complex coupled to the peripheral device and adapted to load a secure driver including program instructions for interfacing with the peripheral device.

27. The computer system of claim 26, wherein the secure driver comprises a digitally signed file.

28. The computer system of claim 26, further comprising a secure program storage device adapted to store the secure modem driver.

29. The computer system of claim 28, wherein the secure program storage device comprises a flash memory.

30. The computer system of claim 28, wherein secure program storage device is located on the peripheral device.

31. The computer system of claim 26, further comprising a computer basic input output system (BIOS) memory adapted to store the secure driver.

32. The computer system of claim 27, further comprising a program storage device adapted to store a public key for authenticating the digitally signed file.

33. The computer system of claim 27, further comprising a system basic input output system (BIOS) memory adapted to store a public key for authenticating the digitally signed file.

34. The computer system of claim 28, wherein the secure program storage device is secured by an authentication key.

35. The computer system of claim 34, wherein the physical layer hardware is adapted to receive the authentication key over the communications channel.

36. The computer system of claim 28, wherein the secure program storage device is secured by a password.

37. A method for protecting a software driver, comprising:

storing a secure driver in a computer system, the secure driver including program instructions for interfacing with a peripheral device;

loading the secure driver; and

interfacing with the peripheral device using the secure driver.

38. The method of claim 37, wherein storing the secure driver comprises storing a digitally signed file.

39. The method of claim 37, wherein storing the secure driver comprises storing the secure driver in a secure program storage device.

40. The method of claim 39, wherein storing the secure driver in the secure program storage device comprises storing the secure driver in a flash memory.

41. The method of claim 37, wherein storing the secure driver comprises storing the secure driver in a secure program storage device located on the peripheral device.

42. The method of claim 37, wherein storing the secure driver comprises storing the secure driver in a computer basic input output system (BIOS) memory in the computer system.

43. The method of claim 38, further comprising storing a public key for authenticating the digitally signed file in the computer system.

44. The method of claim 43, wherein storing the public key for authenticating the digitally signed file comprises storing the public key in a system basic input output system (BIOS) memory in the computer system.

45. The method of claim 37, wherein loading the secure driver comprises loading the secure driver during an initialization of the computer system.

46. The method of claim 39, wherein storing the secure driver in the secure program storage device comprises securing the secure program storage device with an authentication key.

47. The computer system of claim 46, further comprising receiving the authentication key over the communications channel.

48. The computer system of claim 39, wherein storing the secure driver in the secure program storage device comprises securing the secure program storage device with a password.

49. A method for providing a secure driver, comprising:

storing a secure driver, the secure driver including program instructions for implementing a communication protocol;

loading the secure driver; and

communicating data over a communications channel based on the program instructions in the secure driver.

50. The method of claim 49, wherein communicating data over the communications channel includes:

demodulating an incoming analog signal to generate a digital receive signal;

modulating a digital transmit signal to generate an analog transmit signal;

decoding the digital receive signal based on the program instructions in the secure driver; and

encoding the digital transmit signal based on the program instructions in the secure driver.

51. The method of claim 49, wherein storing the secure driver comprises storing a digitally signed file.

52. The method of claim 49, wherein storing the secure driver comprises storing the secure driver in a secure program storage device.

53. The method of claim 52, wherein storing the secure driver in the secure program storage device comprises storing the secure driver in a flash memory.

54. The method of claim 52, wherein storing the secure driver comprises storing the secure driver in a secure program storage device located in a computer.

55. The method of claim 49, wherein storing the secure driver comprises storing the secure driver in a secure program storage device located in an expansion card.

56. The method of claim 49, wherein storing the secure driver comprises storing the secure driver in a computer basic input output system (BIOS) memory in a computer system.

57. The method of claim 49, further comprising storing a public key for authenticating the digitally signed file.

58. The method of claim 57, wherein storing the public key for authenticating the digitally signed file comprises storing the public key in a system basic input output system (BIOS) memory in a computer system.

59. The method of claim 52, wherein storing the secure driver in the secure program storage device comprises securing the secure program storage device with an authentication key.

60. The method of claim 59, further comprising receiving the authentication key over the communications channel.

61. The method of claim 52, wherein storing the secure driver in the secure program storage device comprises securing the secure program storage device with a password.